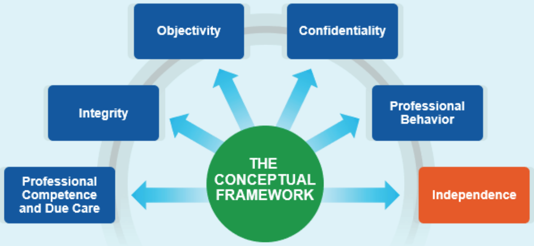
Exploring the IESBA Code: A Focus on Technology

Technology is changing the way that professional accountants (PAs) perform their work. While technological innovations can enhance the scope, efficiency, and effectiveness of this work, they can also pose new challenges in applying the conceptual framework of the IESBA Code ("the Code") to technology-related matters such as artificial intelligence (AI), blockchain, cloud-based computing, and cyber security. The existing Code provides high level, principles-based guidance for most technology-related ethics issues that professional accountants and firms might encounter. As part of its technology initiatives, IESBA is in the process of developing technology-related revisions to the Code.

FOR EXAMPLE: McKay Foods is a major supermarket chain committed to key sustainability goals. The company's annual report sets out a net-zero emissions target and a pledge to end its current practice of sending food waste to landfills—both by 2030. McKay has also committed to extend these goals to their complete supply chain by 2040. McKay relies on blockchain technology to support its supply chain transactions and sustainability reporting, and Internet of Things (IoT) devices to monitor delivery truck fleet information (such as driver details, truck location, and temperature of goods in transit). Further, the company has implemented AI-enabled tools that analyze staff performance reviews to detect evidence of bias, in support of the company's Diversity, Equity & Inclusion Policy.

CONTEXT FOR PAs WORKING IN BUSINESS:

McKay's Chief Sustainability Officer is a PA, and is tasked with monitoring and reporting the appropriate metrics to support the company's ESG initiatives. This is one of the highest profile initiatives for the company, and stakeholder support depends on meeting the company's stated goals.



For more on the Conceptual Framework and the Fundamental Principles see installments 1–5 of Exploring the IESBA Code.

CONTEXT FOR PAs WORKING IN PUBLIC PRACTICE:

A large PA firm provides assurance services to McKay. The firm's cloud service provider has proposed a plan to maintain McKay's IoT data which would centralize McKay's data and make the firm's assurance work more efficient.

THREATS TO COMPLIANCE WITH THE FIVE FUNDAMENTAL PRINCIPLES AND INDEPENDENCE

Artificial Intelligence:

Performance reviews can be prone to unconscious bias, which can result in a self-interest or familiarity threat to objectivity. AI systems are themselves subject to bias, but when used appropriately, AI-enabled tools can also help identify and mitigate these threats.

Blockchain:

New blockchain systems are often tested by running parallel to the legacy system, with reconciliations. Pressure to save costs or even skip this step might give rise to a self-interest threat to objectivity (through over-reliance) and to professional competence and due care. An intimidation threat to integrity might also arise due to internal and stakeholder pressures to meet sustainability goals sooner than later.

Use of IoT devices:

IoT devices are prone to cybersecurity weaknesses. If the firm:

- does not recognize the inherent security risks of IoT devices, this could lead to a self-interest threat to professional competence and due care; or
- assumes that the client is adequately addressing the risks, this could lead to a familiarity threat to confidentiality of client information.

Cloud-Based Storage of Client Data:

Independence might be threatened if the cloud service provider maintains the only copy of the client's IoT-generated data and acts under the direction of the firm.

IFAC International Federation of Accountants®
529 Fifth Avenue, New York 10017
www.ifac.org | +1 (212) 286-9344 | @ifac | company/ifac

IESBA International Ethics Standards Board for Accountants®
www.ethicsboard.org
@ethics_board | company/iesba